

Claims

- [c1] A method of introducing randomness into the process of the dictionary encoding of Lampel-Ziv data compression by shuffling the initial values of the dictionary with the encryption key.
- [c2] A method for combining a random shuffle with a Lampel-Ziv data compression to achieve a simultaneous data compression and encryption, comprised of the following steps:
- a) Use the encryption key to shuffle the initial values of the dictionary randomly.
 - b) Compress the input string normally.
 - c) Perform the bit-wise XOR operation on the compressed result and the encryption key.
- [c3] A method as defined in claim 2, where step a) is comprised of the following step:
- a) If the dictionary doesn't have any initial values, initialize the dictionary with a particular set of values and then use the encryption key to shuffle the dictionary.
- [c4] A cryptographic method of concealing information in the process of Huffman coding by altering the Huffman tree with an encryption key.
- [c5] A method of shuffling the Huffman tree with an encryption key comprised of the following steps:
- a) Associate each interior node with a bit of the encryption key.
- [c6] b) Swap the left child and the right child of an interior node, if the corresponding encryption bit is 1.
- [c7] A method of introducing randomness into the process of the arithmetic coding by shuffling the interval table with an encryption key. That is, a method of introducing randomness into the process of the arithmetic coding by changing the order of dividing an interval into smaller intervals with an encryption key.